Counting “Supersingularity” in Arithmetic Statistics

Wanlin Li, Washington University in St. Louis

Jun 18, 2024

Recall: Chebyshev's bias

Chebyshev (1853): there are more primes equal $4k+3 \leq X$ for most X.

Number of primes $p < X$

X	$p = 4k+1$	$p = 4k+3$
100	11	13
1000	80	87
10000	609	619
26862	1473	1473

Question: Consider $\chi_4(p) = \begin{cases} 1, & p = 4k+1 \\ -1, & p = 4k+3 \end{cases}$, how often is

$$\sum_{p<X} \chi_4(p) < 0?$$

To answer this question, study

$$L(s,\chi) = \prod_p (1 - \chi(p)p^{-1})^{-s}.$$

Recall: Roots of $L(s, \chi)$ and LI

Generalized Riemann Hypothesis (GRH, Piltz 1884):

Any non negative real root $\sigma + it$ of $L(s, \chi)$ satisfies $\sigma = \frac{1}{2}$.

Grand Simplicity Hypothesis/ Linear Independene Conjecture (GSH/LI, Wintner 1938):

The set $\{t \geq 0 \mid L(\frac{1}{2} + it, \chi) = 0\}$ is $\mathbb{Q}$-linearly independent.

Theorem (Rubinstein– Sarnak, 1994)

Under the GRH and GSH/LI, the log density of $\{X \mid \sum_{p<X} \chi(p) < 0\}$ *is*

$$\delta(\chi_4) \approx 99.59\%.$$

Moreover, for any quadratic character χ, $50\% < \delta(\chi) < 100\%$.

Question: What happens when LI fails?

Will we see different prime distribution behavior?

How can LI fail and where to find examples?

LI: The set $\{t \geq 0 \mid L(\frac{1}{2} + it, \chi) = 0\}$ is $\mathbb{Q}$-linearly independent.

Note that one way for LI to fail is $L(s, \chi)$ having a real root at $1/2$.

In the case where χ is a quadratic character over $\mathbb{Q}$, may not exit?

Conjecture (Chowla, 1965)

For any quadratic Dirichlet character χ over $\mathbb{Q}$, $L(1/2, \chi) \neq 0$.

More generally, recall from Youness' talk:

Haselgrove's condition for the modulus q:

For all characters χ modulo q, $L(s, \chi) \neq 0$ for all $s \in (0, 1)$.

Chowla's conjecture is still open and suggests it might be hard to find a counter-example for LI over $\mathbb{Q}$. Over some number fields, Dirichlet character χ with $L(1/2, \chi) = 0$ is known to exist. (Armitage, 1972)

Bailleul (2021): Such fields give examples for reversed bias!

Dirichlet L-functions over $\mathbb{F}_q(t)$

To study order ℓ Dirichlet characters χ over $\mathbb{F}_q(t)$ is equivalent to study cyclic field extensions $L/\mathbb{F}_q(t)$ because

$$\zeta_L(s) = \zeta_{\mathbb{F}_q(t)}(s) \prod_{i=1}^{\ell-1} L(s, \chi^i).$$

In particular, we are interested in fields L whose constant field is $\mathbb{F}_q$. Such an L is a function field of a smooth projective curve $C/\mathbb{F}_q$.

$$\begin{array}{ccc} k(C) & & C \\ {\scriptstyle \mathbb{Z}/\ell\mathbb{Z}} \big\uparrow & & \big\downarrow {\scriptstyle \mathbb{Z}/\ell\mathbb{Z}} \\ \mathbb{F}_q(t) & & \mathbb{P}^1_{\mathbb{F}_q} \end{array}$$

Note that since there are nontrivial maps $\mathbb{F}_q(t) \to \mathbb{F}_q(t)$, there is NOT a canonical map $\mathbb{F}_q(t) \hookrightarrow k(C)$ or a well-defined degree.

Primes of function fields and points on curves

As a global field, the function field $k(C)$ has a set of valuations such that

$$\prod_v |h|_v = 1, \quad \forall h \in k(C).$$

Each v corresponds to a point $P \in C(\overline{\mathbb{F}}_q)$, and

$$|h|_{v_P} = |P|^{-d_P}$$

where d_P is the order of vanishing and $|P|$ is the size of the defining field.

Note that there is no Archimedean place and thus no canonical choice of ∞ or ring of integers.

The zeta function of $k(C)$ is given by

$$\zeta_{k(C)}(s) = \prod_{P \in C(\overline{\mathbb{F}}_q)} (1 - |P|^{-s})^{-1}.$$

The **Weil conjectures** imply that $\zeta_{K(C)}(s)$ can be computed from $|C(\mathbb{F}_q)|, |C(\mathbb{F}_{q^2})|, \cdots, |C(\mathbb{F}_{q^g})|$.

Weil Conjectures and LI for function fields

Weil conjectures:

- $\zeta_C(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$ where $P(q^{-s}) = \prod_{i=1}^{2g}(1-\alpha_i q^{-s}) \in \mathbb{Z}[q^{-s}]$
- $\alpha_i \alpha_{2g-i+1} = q$, for all $1 \leq i \leq g$
- $|\alpha_i| = \sqrt{q}$, roots are of the form $q^s = \sqrt{q}e^{i\theta}$.

Note that for the curve $\mathbb{P}^1$ with function field $\mathbb{F}_q(x)$, its zeta function is

$$\zeta_{\mathbb{P}^1}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$$

If C corresponds to a quadratic extension $K/\mathbb{F}_q(x)$ with character χ, then

$$\zeta_C(s)/\zeta_{\mathbb{P}^1}(s) = L(s,\chi) = P(q^{-s}).$$

LI for χ is equivalent to the multiplicative group generated by

$$\{e^{i\theta_1}, \cdots, e^{i\theta_g}\}$$

having rank g. (Maximal Angle Rank)

Central vanishing $L(1/2,\chi) = 0 \iff \alpha_i = \sqrt{q}$ for some i.

Question: How to find curves with small Frobenius angle rank?

What is supersingularity?

Consider an elliptic curve defined over a finite field $\mathbb{F}_q$ as

$$\mathscr{E} : y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{F}_q.$$

The polynomial of Frobenius is

$$P(q^{-s}) = (1 - \alpha q^{-s})(1 - \beta q^{-s}), \qquad \alpha\beta = q.$$

Weil conjectures $\Rightarrow |\alpha| = |\beta| = \sqrt{q}$, algebraic integer

$\mathscr{E}$ is called **supersingular** if $v_q(\alpha) = v_q(\beta) = \frac{1}{2}$;

$\mathscr{E}$ is called **ordinary** if $v_q(\alpha) = 1, v_q(\beta) = 0$.

For a genus g curve $C/\mathbb{F}_q$ with polynomial

$$P(q^{-s}) = \prod_{i=1}^{g}(1 - \alpha_i q^{-s})(T - \beta_i q^{-s}), \qquad \alpha_i\beta_i = q.$$

Its Jacobian $\mathscr{A}$ is called **supersingular** if $v_q(\alpha_i) = v_q(\beta_i) = \frac{1}{2}$ for all i;

$\mathscr{A}$ is called **ordinary** if $v_q(\alpha_i) = 1, v_q(\beta_i) = 0$ for all i.

Why do we care about supersingularity?

Large Endomorphism:

ordinary $\mathscr{E}/\mathbb{F}_q$ has endomorphism algebra $\mathbb{Q}(\sqrt{-d})$;

for supersingular $\mathscr{E}/\mathbb{F}_q$, a quaternion algebra over $\mathbb{Q}$.

$\mathscr{A}$ supersingular $\iff$ $\mathscr{A} \sim \mathscr{E}_{ss} \times \cdots \mathscr{E}_{ss}$, thus very large $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathscr{A}) \otimes \mathbb{Q}$!

Extreme point counting:

Over $\mathbb{F}_{p^2}$, the elliptic curve with minimal and maximal number of $\mathbb{F}_{p^2}$-points are supersingular. Curves with supersingular Jacobians can have extreme point counting.

Multiplicative relation among eigenvalues:

$\mathscr{A}$ supersingular $\iff$ every eigenvalue $\alpha_i = \mu\sqrt{q}$ satisfying $\mu^n = 1$.

Jac(C) supersingular = maximally violating LI!

Moreover, over $\mathbb{F}_{q^n}$, we get central vanishing as the unique root.

Central vanishing $\iff$ Jacobian having a supersingular factor.

Exceptional bias on prime distribution from "supersingularity"

Devin–Meng (2021): the quadratic character over $\mathbb{F}_9(t)$ corresponding to the **supersingular** curve

$$y^2 = x^4 + 2x^3 + 2x + (\sqrt{3})^7$$

has the property that $\delta(\chi) = 100\%$.

Theorem (Bailleul–Devin–Keliher –L., 2023)

For any χ with $\delta(\chi) = 100\%$, the Jacobian of the corresponding curve admits a supersingular isogeny factor.

Cha (2008): the quadratic character over $\mathbb{F}_5(t)$ corresponding to the **supersingular** curve

$$y^2 = x^5 + 3x^4 + 4x^3 + 2x + 2$$

has the property that $\delta(\chi) < 50\%$, bias in the "wrong" direction.

Theorem (Bailleul–Devin–Keliher –L., 2023)

For any square q, there exists a supersingular genus 2 curve corresponding to a quadratic character satisfying $\delta(\chi) < 50\%$.

Different ways to count "supersingularity"

"Question": How to count "supersingularity"?

Choose a "family" $\mathcal{S}$, study the density of "supersingular" $\mathscr{A}$ in "family".

1. **large q limit:** $\mathcal{A} \to \mathcal{S}$ algebraic family over $\mathbb{F}_p$, for "supersingular" $\mathscr{A} \in \mathcal{S}(\mathbb{F}_{p^n})$, study its density over $|\mathcal{S}(\mathbb{F}_{p^n})|$ as $n \to \infty$.

   comment: Not changing $\mathcal{S}$ in the process, study the geometry of the "supersingular" locus in $\mathcal{S} \otimes \overline{\mathbb{F}}_p$.

2. **large g limit:** When $\mathcal{S}$ is not an algebraic family (e.g. hyperelliptic Jacobians), fix $\mathbb{F}_q$ and consider $\mathscr{A}/\mathbb{F}_q$ in the family with dimension $\leq g$, study the density of "supersingular" objects as $g \to \infty$.

   comment: close to counting in number fields, Cohen–Lenstra type

3. **Reduction:** $\mathcal{A} \to \mathcal{S}$ algebraic family with $\mathcal{S} = \operatorname{Spec} \mathcal{O}$ where $\mathcal{O} = \mathbb{Z}$ or $\mathbb{F}_q[t]$, for $p \in \mathcal{O}$ with height $\leq X$, study the density of "supersingular" $\mathscr{A}/k_p$ as $X \to \infty$.

   comment: study Galois representation of $\mathcal{A}[\ell^\infty]$

How to find/construct supersingular curves?

- Honda–Tate theory for low genus case
- Shimura–Taniyama theorem for high genus case

Recall: supersingular $\mathscr{A}$ has larger $\mathrm{End}^0_{\mathbb{F}_p}(\mathscr{A})$, conversely endomorphism forces $\mathscr{A}$ to be more "supersingular".

Shimura–Taniyama (1961): The "supersingularity" of $\mathcal{A}$ mod p with CM by (E, ϕ) is determined by the behavior of p in the extension $E/\mathbb{Q}$.

Example: An elliptic curve E over a number field L with CM by $K = \mathbb{Q}(\sqrt{-D})$, E mod $\mathfrak{p}$ is ordinary at a prime $\mathfrak{p} \subset L$ above $p \subset \mathbb{Q}$ if and only if p splits in $K/\mathbb{Q}$.

The curve $y^2 = x^3 - 1$ is supersingular over $\mathbb{F}_p$ for any $p \equiv 2 \bmod 3$.

Example: Jacobian of $y^\ell = x(x-1)(x+1)^{\ell-2}$ is supersingular if p is inert in $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$.

Counting "supersingularity": large q limit

Consider an elliptic curve defined as

$$\mathscr{E} : y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{F}_q$.

Question: What is

$$\lim_{q \to \infty} \frac{|\{A, B \mid \mathscr{E} \text{ is supersingular}\}|}{q^2} \ ?$$

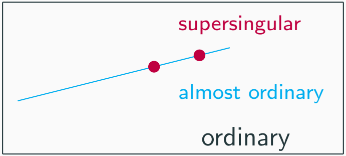
Answer: 0

When vary the parameters $A, B \in \overline{\mathbb{F}}_p$, the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is $\approx \frac{p}{12}$.

$X_0(1)_{\overline{\mathbb{F}}_p}$

The geometry of “supersingular” locus

The p-adic valuation of $\alpha_1, \cdots, \alpha_{2g}$ form a poset and this gives a (Newton) stratification of $\mathcal{A}_g/\overline{\mathbb{F}}_p$. (Oort, 2001)



$\mathcal{A}_2$ over $\overline{\mathbb{F}}_p$
$\dim \mathcal{A}_2 = 3$

The geometry of various Newton locus in Shimura varieties have been studied by Chai, Oort, Fox, Howard, Pappas, Vollaard, Wedhorn, $\cdots$

Open problem: which Newton locus contain Jacobians of (hyperelliptic) curves?

This problem had been studied by many authors.

(See a survey by Pries: Current results on Newton polygons of curves)

Can use curves with large automorphism group to force “supersingular”.

Counting "supersingularity": large g limit

Cais–Ellenberg–Zureick-Brown (2012): described a probability distribution of principally quasi-polarized p-divisible groups ($\mathscr{A}[p^\infty]$), computed the distribution of discrete invariants from this distribution, obtained a heuristic analogous to conjectures of Cohen-Lenstra type.

They carried out numerical investigation and found the proportion of ordinary plane curves over $\mathbb{F}_3$ seems to agree with thee heuristic while hyperelliptic curves over $\mathbb{F}_3$, plane curves over $\mathbb{F}_2$ seem not.

Sankar (2019): proved the density of ordinary Artin-Schreier curves $y^p - y = f(x)$ over $\mathbb{F}_q$ and superelliptic curves $y^\ell = f(x)$ over $\mathbb{F}_{2^n}$ do not obey the CEZB heuristic.

Garton–Thunder–Weir (2024): extended CEZB, described an alternative model which matches the data for hyperelliptic curves defined over $\mathbb{F}_{3^n}$.

Counting "supersingularity": reduction

Question: Given an elliptic curve E over a number (global) field L, what's the density of p satisfying (E mod p) ordinary/supersingular?

Complete answer for CM case: By Shimura–Taniyama (1961), if E/L has CM by $K = \mathbb{Q}(\sqrt{-D})$, then E has ordinary reduction at primes $q \subset L$ above $p \subset \mathbb{Q}$ when p splits in $K/\mathbb{Q}$. (**congruence condition**)

Conjecture (Lang–Trotter, 1976): When $E/\mathbb{Q}$ is not CM, the set of supersingular primes for E with height $\leq X$ has density $\approx \sqrt{X}/\log X$.

Theorem (Serre, 1977): For any elliptic curve E over a number field L without CM, its set of ordinary primes has density 1.

Theorem (Elkies, 1987) For any elliptic curve $E/\mathbb{Q}$, there exist infinitely many supersingular primes.

Positive density of ordinary primes

Conjecture (Serre): For any abelian variety A of dimension g over a number field L, the density of ordinary primes is positive.

(**Chebotarev's density**?)

Theorem (Katz, 1982; Sawin, 2016): For $g = 2$, the set of ordinary primes has density 1, $\frac{1}{2}$ or $\frac{1}{4}$. The later two cases could only occur for A with a CM isogeny factor and the density becomes 1 after a finite field extension.

More results by Noot, Pink, Fité, $\cdots$

Still unknown for a generic abelian threefold.

Theorem (Cantoral Farfán–L.–Mantovan–Pries–Tang, 2023)
Conjecture holds for the Jacobian of $C : y^5 = x(x-1)(x-t)$.

And this density is 1 over $L(\zeta_5)$.

Strategy on Density of Ordinary Primes

- Given $L/\mathbb{Q}$, the set of q above a split prime $p \subset \mathbb{Q}$ has density 1. Thus, it suffices to consider the set of split primes and $A/\mathbb{F}_p$.

- For an elliptic curve $\mathscr{E}/\mathbb{F}_p$ with $p > 2$, it is ordinary when $p \nmid a$. By the Hasse bound, $|a| \leq 2\sqrt{p}$. Thus, $\mathscr{E}$ ordinary $\iff a \neq 0$.

  This a is an invariant of the Frobenius which
  1. asserts $\mathscr{E}$ ordinary;
  2. takes finite integral values for non ordinary $\mathscr{E}$ independent of p.

  For an abelian surface $\mathscr{S}/\mathbb{F}_p$ with characteristic polynomial $x^4 - a_1x^3 + a_2x^2 - pa_1x + p^2$, it is ordinary if $p \nmid a_2$. Since $|a_2| \leq 6p$, $\mathscr{S}$ ordinary $\iff a_2/p \notin \{-6, \ldots, 6\}$.

  This step defines a function on the ℓ-adic monodromy group such that the density of ordinary primes is bounded below by the ratio of connected components on which this function is non-constant. (Chebotarev's density)

Strategy on Density of Ordinary Primes

- Study connected components of the ℓ-adic monodromy group.

  The elliptic curve case follows from Serre's open image theorem.

  Sawin's result relies on the work of Fité–Kedlaya–Rotger–Sutherland (2012) on the Sato–Tate groups of abelian surfaces.

- For a Jacobian $\mathrm{Jac}(C)/L$ in the family

  $$C : y^5 = x(x-1)(x-t),$$

  because of its nontrivial endomorphism, for $p \neq 5$, it has two possible Newton polygon types, μ-ordinary and basic.

  We define functions on Frobenius based on its image in $\mathrm{Gal}(L(\zeta_5)/L)$ which assert μ-ordinary reduction.

  Note that the ℓ-adic monodromy group is connected over $L(\zeta_5)$ and the Mumford–Tate Conjecture (Vasiu, 2008) holds. We conclude:

  Theorem(CLMPT): The set of μ-ordinary primes has density 1.

Infinitude of Supersingular Primes

Theorem (Elkies, 1987, 1989)

For every elliptic curve $E/\mathbb{Q}$ (a large set of number fields), there exist infinitely many primes at which the reduction of E is supersingular.

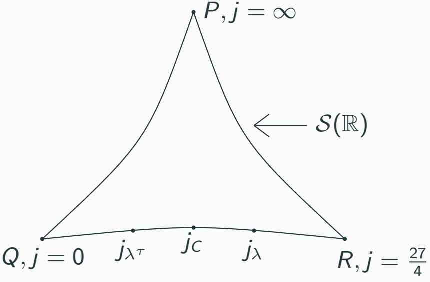
Remark: Analogous results for certain abelian surfaces were obtained by Jao (2003), Sadykov (2004), and Baba-Granath (2008).

Theorem (L.–Mantovan–Pries–Tang, in progress)

Let $C : y^5 = x(x-1)(x-t)$ be a smooth projective curve satisfying:

- $j_C := \frac{(t^2-t+1)^3}{t^2(t-1)^2} \in \mathbb{Q} \cap [0, \frac{27}{4}]$;
- *the reduction of C at 5 is singular;*

then there exist infinitely many basic primes of $\mathrm{Jac}(C)$.



Thank you for your attention !